NMCI DEMONSTRATION

1. OVERVIEW

The Offerors shall provide a demonstration of a currently-managed infrastructure that provides services similar as those proposed to the Government. Offerors shall highlight the areas of its demonstrated infrastructure which differ from those proposed under this solicitation. For those highlighted areas, offerors should describe how it will modify the demonstrated infrastructure to meet the requirements of NMCI. Demonstrations will take place at the offeror's facilities, and will not exceed two days. Offerors should provide a separate room, suitable for private deliberations, for Government evaluators to use during the demonstration process. Offerors will be notified of the date its demonstration evaluation will commence.

At a minimum, the demonstration shall include the following areas:

- Interoperable Data, Voice, Video Services
- Help Desk and Maintenance
- Network Operations and Management
- Security
- Invoicing, Ordering, and Billing

2. OBJECTIVES

The objectives of the Demonstration are as follows:

- To assess the Offeror's capability to provide services of the scope, magnitude and complexity of the NMCI services procurement.

- To independently verify the offeror's ability to achieve service levels reflective of those set forth in its proposal and to demonstrate security effectiveness.

3. PRE-AWARD DEMONSTRATIONS

3.1 Performance

The Offerors shall explain and provide data regarding how its proposed demonstration systems currently meet SLAs similar to those presented in Attachment 2 of the solicitation. This data should be captured and provided to the Government during demonstrations. The offeror shall provide a sample report that reflects achievement of representative SLAs.

3.2 Services

This demonstration shall include services similar to the data, voice, and video seats defined in the solicitation. The demonstration shall address responsiveness, capacity, availability, interoperability, and information assurance for each service.

3.3 Security

The security demonstration should show how layered defenses are incorporated within the overall architecture, and the offeror's intrusion detection, firewall, and virtual private network approach. The offeror should provide an example of how it provides intrusion detection data to its current customers. Additionally, the offeror shall provide a copy of an existing System Security Authorization Agreement (SSAA) for a program similar to NMCI. The offeror should address the following areas as part of the security demonstration of the infrastructure, if it applies to its current operations and service offerings.

Operating System Security: The Offeror shall demonstrate how the chosen operating systems will be securely configured for voice, video, and data components.
Legacy Systems Connectivity: The Offeror will demonstrate how it will mitigate the risks involved with connections to legacy systems that will remain in the NMCI. This should include demonstrating the use of VPNs if required for legacy system connectivity.
Remote User Connectivity: The Offeror will demonstrate how remote users will have access to the NMCI including the use of Information Assurance (IA) mechanisms.
Firewall and Intrusion Detection System (IDS) Configuration and Implementation: The Offeror will demonstrate how it will integrate IDS's and maintain attack signatures up to date. This should include a plan of action for updating Firewalls, IDS's, and other network security components across the enterprise upon detection of a network intrusion.
Anti-Virus Verification: The Offeror will demonstrate how it will maintain up to date Virus signatures across the enterprise.
Incident Reporting and Response: The offeror will demonstrate its plan for incident reporting and response.
Denial of Service Attacks: The offeror will demonstrate IA mechanisms and procedures used to defend against distributed denial of service attacks and network signaling attacks.
Disaster Recovery: The offeror will demonstrate its plan for disaster recovery.
PKI and Smart Card: The offeror will demonstrate how it provides PKI functionality to its current users. This will include certificate issuance, revocation, authentication, and Certificate Revocation List (CRL) maintenance. Use of smart cards to provide access control can also be demonstrated, if currently used.
Information Assurance Vulnerability Alert (IAVA)/Information Operations Condition (INFOCON): The offeror will demonstrate how IAVAs and INFOCON changes will be processed.

3.4 Help Desk

Help desk and maintenance demonstration shall include: help desk operations, software, processes and procedures, upgrade procedures, customer satisfaction monitoring and reporting, and performance monitoring and reporting.

3.5 Network Operations and Management

Network operations and management demonstration may include automated asset inventory management, fault isolation, data archiving, correction procedures, enterprise software distribution, hardware distribution, capacity planning and management, configuration management, external network gateways, and end-to-end performance monitoring and reporting. These demonstrations of network management services may be representative of data, voice, and video services delivery comparable to proposed NMCI offerings.

3.6 Ordering and Invoicing

If currently used, the Offeror shall provide a demonstration of a software application that provides for electronically placing orders, receiving and processing bills/invoices, and viewing order status and financial status from remote sites. The demonstration should include the process of obtaining electronic signatures and approval routing.

4. DEMONSTRATION PLAN

The Offeror shall prepare a Demonstration Plan that provides the Government with a comprehensive agenda, checklist for all items that will be demonstrated, and sufficient background detail to provide evaluators with an understanding of the architecture and operational procedures to be demonstrated.